Windows - Local recon

System information

```
systeminfo
```

All hotfixes applied

```
Get-WmiObject -Class Win32_QuickFixEngineering -ComputerName .
```

OS Information

```
Get-WmiObject -Class Win32_OperatingSystem -ComputerName .
```

Logon Sessions

```
Get-WmiObject -Class Win32_LogonSession -ComputerName .
```

Logged on users

```
Get-WmiObject -Class Win32_ComputerSystem -ComputerName .
```

Services

```
Get-WmiObject -Class Win32_service -ComputerName .

Get-WmiObject -Class Win32_service -ComputerName . | Where-Object { $_.State -eq "Running" }

# Returns Name, service account, a description and the path to the executable
Get-WmiObject -Class Win32_service -ComputerName . | Select Name,StartName,Description,PathName
```

Local users, groups and memberships

```
Get-LocalUser
Get-LocalGroup
Get-LocalGroupMembership <groupname>
```

Get listening services

```
netstat -a -n -o
```